REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-15, 18-24, 26, and 27 are pending in the present application, Claims 1-15 and 18-24 having been amended, Claims 26 and 27 having been added, and Claim 25 having been canceled. Claims 1-15 and 18-24 are amended to more clearly describe and distinctly claim the subject matter regarded as the invention. Support for the amendments to Claims 1, 5, 11, and 15, and new Claims 26 and 27 is found, for example, in Figs. 1-3, and in the specification at page 6, lines 27-31, page 8, lines 17-22, and page 10, lines 16-21. Applicants respectfully submit that no new matter is added.

In the outstanding Office Action, Claim 25 was rejected under 35 U.S.C. §112, first paragraph; and Claims 1-5, 8-15, and 18-25 were rejected under 35 U.S.C. §103(a) as unpatentable over Mirsa et al. (U.S. Patent No. 5,757,920, hereinafter Mirsa) in view of Haber et al. (U.S. Patent No. 5,781,629, hereinafter Haber),

With respect to the rejection of Claim 25 under 35 U.S.C. §112, first paragraph, Applicants respectfully submit that this ground of rejection is moot in view of the cancellation of Claim 25.

In a non-limiting embodiment of the claimed invention, an originator sends a secured random number to a receiver as part of a login key. Upon reception of this login key, it is possible for the receiver to avoid a multiple use of the login key, even before the expiration of the temporal validity of the login key, by checking a key table.

The receiver stores the secure random number, received as part of the login key, until the key expires. Key expiration is determined by the temporal validity information, which is also transmitted as part of the login key. A quick search of the key table by the receiver

allows the receiver to check for duplicate keys. If a duplicate key is found, then the receiver can stop the communication.

With respect to the rejection of Claim 1 as unpatentable over the combination of Mirsa and Haber, Applicants respectfully submit that the amendment to Claim 1 overcomes this ground of rejection. The combination of Mirsa and Haber do not disclose or suggest the claimed "wherein the keyed hashing technique uses random data that is stored by the destination in a table during the temporal validity of the data."

On the contrary, Mirsa does not disclose or suggest maintaining a list of currently used secure random numbers for eliminating multiple uses of a login key. Mirsa only discloses that multiple use of a copied ticket or login key can be prevented by including a time stamp.[1]

Fig. 2A of Mirsa shows an example of a logon certificate. As shown by Fig. 2, the logon certificate does not include random data that is stored by the destination in a table during the temporal validity of the data. Although Mirsa disclose using a random encryption key, at col. 6, lines 5-7, to encrypt the logon certificate, this random encryption key does not equate to the claimed "wherein the keyed hashing technique uses random data that is stored by the destination in a table during the temporal validity of the data."

Furthermore, Applicants respectfully submit that Haber does not cure the above-noted deficiency in Mirsa. Haber discloses using a time stamp to validate that a given certificate was computed for a given document at the time claimed.[2] The aim of Haber is to provide an improved digital time-stamping system.[3] Haber does not disclose or suggest maintaining a list of currently used secure random numbers for eliminating multiple uses of a login key.

---

[1] Mirsa, col. 7, lines 50-52.
[2] Haber, col. 1, line 66 to col. 2, lines 4.
[3] Haber, col. 3, lines 39-40.

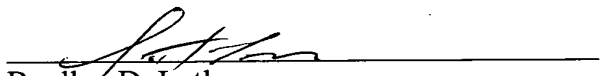
In view of the above-noted distinctions, Applicants respectfully submit that Claim 1 (and Claims 2-4, 20, 22, 26, and 27 dependent thereon) patentably distinguish over Mirsa and Haber, taken alone or in proper combination.

Independent Claims 5, 10, 11, and 15 also recite "wherein the keyed hashing technique uses a random data that is stored by the destination in a table during the temporal validity of the data." As characterized above, Mirsa and Haber fail to disclose or suggest this element of Claims 5, 10, 11, and 15. Accordingly, Applicants respectfully submit that Claims 5, 11, and 15 (and Claims 8, 9, 12-14, 18, 19, 21, 23, and 24 dependent thereon) patentably distinguish over Mirsa and Haber, taken alone or in proper combination.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Joseph Wrkich
Registration No. 53,796

Scott A. McKeown
Registration No. 42,866

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)

I:\ATTY\JW\282839US\282839US-AM.DOC